INTERNET ACCEPTABLE USE POLICY

1. Aim of this policy

The aim of this Acceptable Use Policy (AUP) is to ensure that pupils will benefit from learning opportunities offered by the school's internet resources in a safe and effective manner. Internet use and access is considered a school resource and privilege. Therefore, if the school AUP is not adhered to this privilege will be withdrawn and appropriate sanctions will be imposed.

It is envisaged that the school and parent representatives will revise the AUP as deemed necessary. Before signing, the AUP should be read carefully to indicate that the conditions of use are accepted and understood.

Due to emergency school closures from March 2020, during the COVID-19 pandemic, we have made changes to our teaching and learning approaches to facilitate online learning practices. This updated document provides guidance for the school community on these changes.

2. General Strategies

-Internet sessions in school will always be supervised by a teacher.

-Safe-surfing settings, on school devices, will be used in order to minimise the risk of exposure to inappropriate materials.

-The school will regularly monitor internet usage in school.

-Pupils and teachers will be provided with training in the area of 'Internet safety and Digital Citizenship'.

-Uploading and downloading of non-approved software is not permitted.

-Anti-Virus software will be used and updated as necessary.

-The use of personal memory sticks in school requires a teacher's permission.

-Students and staff will observe good "netiquette" at all times. They will not undertake any actions that may be considered disrespectful to members of the school community, or bring the school into disrepute (See Appendix 1).

-School staff has access to all files used on school computers, including e-mail messages sent and received by pupils.

-School devices may record details of what pupils have viewed on the internet. These records may be reviewed by school staff.

-With Broadband, NCTE provide content filtering which allows access to educational, cultural and general interest sites only. Access to any illegal, obscene or objectionable material will be blocked.

3. World Wide Web

-Pupils or staff will not intentionally visit internet sites that contain obscene, illegal, hateful or otherwise objectionable materials.

-Pupils will use the internet for educational purposes only.

-Pupils and staff will be educated regarding copyright issues relating to online materials.

-Pupils will never disclose or publicise their own or others personal information

-Pupils or staff will be aware that any internet usage may be monitored for unusual activity, security and/or network management reasons.

-Pupils will never arrange a face-to-face meeting with someone that they have "met" on the internet.

4. E-mail

-Senior classes may be allowed to occasionally use e-mail under supervision of teacher for school projects only.

-Personal details will not be revealed (i.e. student's own details or those of others). -Illegal,

obscene, defamatory, annoying or intimidating material are blocked.

-Students will never arrange a meeting with someone they only know through e-mails or internet.

-Attachments will only be sent or received with permission of teacher/computer teacher.

-Pupils or staff will not intentionally send or receive any material that is illegal, obscene or defamatory or that is intended to harm or intimidate another person.

-Pupils must have permission to send and open email attachments.

5. Social Networking/ Website

-Pupils, in consultation with their teachers, will be given the opportunity to publish their work through the school social media sites (e.g. school website, blog and the school social media outlets)

-The publication of student work will be coordinated by a teacher.

-Pupil's work will appear in an educational context on school sites (See appendix 2).

-Digital photographs, audio or video clips of individual students will not be published on the school sites. Instead these will focus on group activities. Individual pupils will not be identified by name.

-Photos or videos showing pupils' faces individually will not be published on social media with the exception of pre-approved sites such as Music Generation and the Parents Association Facebook Page and Instagram Parents Association Facebook Page. This will be done with signed consent from families (See appendix 2)

-Pupil's home address and contact details will be omitted from school social media posts.

-Pupils will continue to own the copyright on any work published.

-Regularly during the school year, parents are requested not to share any photos of other people's children on their social media, without permission. This includes photos which they may take themselves at school events, or photos shared by the school.

6. Mobile Phones

-Due to the dangers of inappropriate use, mobile phones are not permitted in Scoil Mhuire Lourdes.

7. Internet Discussion

-Students will only have access to discussion forums or other electronic communication forums that have been approved by the school.

-Discussion forums and other electronic communication forums will only be used for educational purposes and will always be supervised.

8. Legislation

There is no specific legislation governing Internet safely at school level. Complicating this issue is the fact that the Internet functions in a global context whereas the law operates in a localised one. There are, however; a number of legislations that have relevance to Internet safety. Copies of each of these Acts can be found online. All teachers, students and parents should familiarise themselves with these Acts. They are briefly described as follows:

The Child Trafficking and Pornography Act 1998: This Act legislates against anyone who knowingly produces, prints, publishes, distributes, exports, imports, shows, possesses or sells child pornography. http://www.irishstatutebook.ie/1998_22.html

Interception Act 1993: (The Interception of Postal Packets and Telecommunications Messages Regulation Act 1993). This Act stipulates that telecommunication messages can be intercepted for the purpose of an investigation of a serious offence. Authorisations are subject to certain conditions. http://www.irishstatutebook.ie/1993_10.html

Video Recordings Act 1989: The 1989 Video Recordings Act prohibits the distribution of videos which contain obscene or indecent material which may lead to the depravation or corruption of the viewer. http://www.irishstatutebook.ie/ZZA22Y1989.html

The Data Protection Act 1988 and Data Protection (Amendment) Act 2003: This Act was passed in order to deal with privacy issues arising from the increasing amount of information kept on computer about individuals. http://www.irishstatutebook.ie/ZZA25Y1988.html

9. Support Structures

-Internet Safety Week

-Lessons will be taught each year on Safe Internet Use and Cyberbullying in Senior Classes.

-The school will inform students and parents of key support structures and organisations that deal with illegal material or harmful use of the Internet.

-Information will be sent to parents/guardians regarding safe use and monitoring of children's use of internet at home.

10. Digital Harassment

Every member of staff in Scoil Mhuire Lourdes is issued with a school email address. This address is accessible to all. This allows anyone to email a staff member, which can carry a number of risks to a staff member's dignity at work. In light of this, the following ground rules apply.

- There should be a period of 5 school days allowed for a response to an email. (If the staff member is away, he/she can enable a "Vacation Responder" to let the sender know that they are out of the office and when to expect a response or instructions as to who to direct their email to.)
- Staff are not expected to check their email after hours. Staff are instructed not to give themselves access to their school email after hours on their personal devices. The Board cannot be responsible if staff check emails after hours.
- Emails sent by and to staff members should be in a respectful tone. A staff member is entitled not to respond to an email that they, themselves, deem to be disrespectful in tone. It is recommended that a staff member that receives an email like this arranges to meet a parent face-to-face rather than responding to the content of the email.
- "Mailbombing," the excessive sending of emails to a staff member falls under this policy. All users of email should be aware that, despite best intentions, their actions may cause distress to their colleagues. This can come in a number of forms:
    - Excessively forwarding on resources, links or information
    - Using Reply to All, where it is not appropriate
    - Excessive contact from an individual, e.g. checking in on a child everyday unless explicitly agreed.
- Unsolicited email (or spam). The school uses Google's services to reduce the volume of spam sent to staff members. The email application recommended by the school contains facilities to report spam. The Board cannot be responsible for any spam that arrives in a staff member's inbox.
- Any form of email that falls under the definition of harassment will be treated in the same manner as any other form of harassment.

Other Forms of digital harassment

In the digital age, it is expected that staff are aware of their own online presence and they should adhere to the guidelines of the Teaching Council's Professional Standards. However, staff are entitled to a private life online and this should be respected. For example, a staff member should not feel under pressure to "friend" another member of staff or a parent or anyone else in the

school community. Further guidelines on this can be found in the school's Dignity At Work and Equal Opportunity policy.

11. Sanctions

Misuse of the Internet may result in disciplinary action, including written warnings, withdrawal of access privileges and, in extreme cases, suspension or expulsion. The school also reserves the right to report any illegal activities to the appropriate authorities (See Appendix 3).

Appendix 1
'Netiquette'

Guidelines for good online communication in Scoil Mhuire Lourdes

1. Under no circumstances can pictures or recordings be taken of video calls.
2. Staff, families and students are expected to behave in an appropriate, safe, respectful and kind manner online.
3. It is the duty of parents/guardians to supervise children while they are working online and to ensure any content which they are submitting to their teacher is appropriate.
4. Staff members can communicate with pupils and their families via school emails or through an established app (eg. Zoom)
5. Any electronic forms of communication will be for educational purposes and to allow for communication with families.
6. Students and staff will communicate using tools which have been approved by the school and of which parents have been notified
7. Parental permission will be acquired before setting up a profile for a pupil on a communication forum.
8. For video/Zoom calls, parental permission is implied, as the link to a video call will be communicated via the parent/guardian's email address. Essentially, by virtue of the pupil logging on to the call, permission is assumed.
9. For security reasons, passwords will be provided to families, where applicable.
10. Scoil Mhuire Lourdes cannot accept responsibility for the security of online platforms, in the event that they are hacked.
11. Communication using a mobile phone will not be frequent, but in the rare exception where it is necessary, staff members will ensure that their caller ID is private.

Guidelines for staff members using online communication methods:

1. Under no circumstances can pictures or recordings be taken of video calls.
2. Staff members will communicate with pupils and families during school hours where possible.
3. Staff members will have high expectations regarding pupil behaviour, with any communication which takes place online.
4. Staff members will seek to become familiar with apps before using them with pupils.
5. Staff will check that consent has been given, before setting up a pupil profile for an online app.
6. Staff members will report any concerns regarding online behaviour or interactions to school management.
7. Staff are encouraged to generate a new meeting ID and password for each Zoom meeting being held.
8. Staff members will notify parents/guardians of the date, time and password for a video call via email.
9. Staff members will only admit participants to video conferences, if they recognise the email address/username as being connected to a pupil.

Rules for pupils using online communication methods:

For submitting learning:

1. Submit work and pictures that are appropriate - have an adult take a look at your work before you send it.
2. Use kind and friendly words.

For video calls/Zoom:

1. Pictures or recordings of the video call are not allowed.
2. Remember our school rules - they are still in place, even online.
3. Set up your device in a quiet space, with no distractions in the background.
4. Join the video with your microphone muted.
5. Raise your hand before speaking, just like you would do in class.
6. If you have the chance to talk, speak in your normal voice, using kind and friendly words.
7. Show respect by listening to others while they are speaking.
8. Ensure that you are dressed appropriately for the video call.
9. Be on time - set a reminder if it helps.
10. Enjoy! Don't forget to wave hello to everyone when you join!

Appendix 2

Please review the school Internet Acceptable Use Policy, sign and return this permission form to the school

Dear Parent/Guardian,

As part of the school's programme we offer pupils supervised access to the Internet.

This will allow pupils vast educational opportunities, e.g. helping them to access a wide range of resources, communicate with subject experts and participate in school projects locally and globally. Pupils will also learn valuable skills which may be useful for their future careers.

The Internet is a global computer network which is not controlled by any organisation. This means that information may change, disappear and be controversial or potentially harmful. Although the school actively seeks to promote safe use of the internet, it recognises the possibility that students may accidentally or deliberately access objectionable material.

Usage to the Internet requires responsibility on the part of the user and the school. These responsibilities are outlined in the school Acceptable Use Policy. It is, therefore, important that the enclosed policy is carefully read and signed by the pupils and a parent or guardian. You can find our Acceptable Use Policy on the school website at this link www.smltullow.ie under the Policies tab.

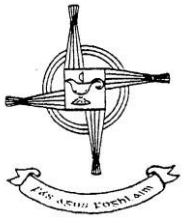
We appreciate that parents and guardians are responsible for setting the standards that their children should follow when using technology. To that end, the school supports and respects each family's right to decide whether or not to allow access to the Internet as defined by the school's Acceptable Use Policy.

Yours Sincerely,

_____

Marie Coen

School Principal.



Internet Use Permission Form – Parents and Pupils

Please review the school Acceptable Use Policy (AUP), discuss it with your child, and sign and return this permission form.

Name of Pupil: _____ Class: _____ **Pupil:**

I agree to follow the school's AUP on the use of the Internet. I will use the Internet in a responsible way and obey all the rules explained to me by the school.

Pupil's Signature: _____ Date: _____

Parent/Guardian:

As the parent or legal guardian of the above pupil, I have read the AUP and grant permission for my child to access the Internet. I understand that Internet access is designed for educational purposes. I also understand that every reasonable precaution has been taken by the school to provide for online safety but the school cannot be held responsible if pupils access unsuitable websites.

Signature: _____ Date: _____

Publishing pupils' photos, videos or work online:

I understand that, if the school considers it appropriate, my child's photo, video or schoolwork may be chosen for inclusion on the school's social media (e.g. website, blog, social media outlet or other educational learning platform) in keeping with the terms of the school Acceptable Use Policy.

I understand and accept the terms of the AUP relating to publishing children's images or work online.

Signature: _____ Date: _____

Appendix 4

Protocol in the event of an incident during a Zoom session

- Behaviour-pupil/parent/adult
- Child Protection Concern
- Disclosure

Remember that as a staff we are mandated to report incidents of Child Protection when engaging in remote teaching and online learning.

1. React calmly.

2. Inform the pupils that unfortunately that the session must end.

3. Reassure them that there will be another session scheduled and their parents will receive the invite soon.

4. Breaches of the Code of Behaviour or inappropriate behaviour must be reported to the Principal and will be dealt with thereafter.

5. In such instances, children may be excluded from further meetings of this nature and parents may be contacted and informed.

6. In the event if a child protection issue, staff members should inform the school's DLP if they notice, or have any concerns or should a disclosure be made to them. If the DLP is not available, contact the DDLP. Record details of incident.

7. Please end the session at any time should you deem any content inappropriate.